Yong-Sheng Zhang, Chuan-Feng Li*, Guang-Can Guo†
Laboratory of Quantum Communication and Quantum Computation, Department of Physics, University of Science and Technology of China, Hefei 230026, People's Republic of China

An unconditionally secure quantum cion tossing protocol for two remote participants via entangled swapping is presented. The security of this protocol is guaranteed by the nonlocal property of quantum entanglement and the classical complexity.

PACS number(s): 03.67.Dd, 03.65.Ud, 89.70.+c

I. INTRODUCTION

Quantum cryptography is a field which combines quantum theory with information theory. The goal of this field is to use the laws of physics to provide secure information exchange, in contrast to classical methods based on (unproven) complexity assumption. Since the publication of BB84 protocol, quantum key distribution (QKD) [1,2] has developed into a well understood application of quantum mechanics to cryptography. In particular, quantum key distribution protocols became especially important due to technological advances which allow their implementation in the laboratory [3]. Besides QKD, quantum cryptography has many other applications, such as quantum bit commitment, quantum coin tossing (QCT), quantum secret sharing, quantum secure computation, oblivious transfer of quantum cryptography and quantum gambling [4], etc. However, Mayers [5] and Lo and Chau [6] have shown that ideal quantum bit commitment is insecure. Their work also raised serious doubts on the possibility of obtaining any secure two-party protocol, such as oblivious transfer and coin tossing.

Coin tossing is defined as a method of generating a random bit over a communication channel between two distant parties. The parties, traditionally named Alice and Bob, do not trust each other, or a third party. They create the random bit by exchanging quantum and classical information. At the end of the protocol, the generated bit is known to both of them. Coin tossing can be done in classical cryptography either through trusted intermediaries or by accepting some unproven computational assumptions [7]. However, it is interesting whether quantum mechanics can provide secure coin tossing protocol without assistance of intermediaries.

*Electronic address: cfli@ustc.edu.cn
†Electronic address: gcguo@ustc.edu.cn

A coin tossing protocol is said to be ideal if the probability that the result accepted by both parties without cheating is exact one, and both outcomes 0 and 1 occur with equal probability of 1/2. Lo and Chau proved that the secure ideal coin tossing protocol is impossible [8], and it does not matter whether the protocol is purely quantum, classical or quantum but with measurements. However, the unconditionally secure protocols of non-ideal QCT have been proposed [9,10] and it was shown that coin tossing is strictly weaker than bit commitment [11]. As denoted in [9], in the non-ideal case, it is requested that, for $b = 0, 1$, the probability that Alice gets bit b and passes the test is smaller than $1/2$ whatever she does, and similarly for Bob. If the bound $1/2$ perfectly against any of the two participants, the task realized is called an *exact* coin tossing. If the bound is actually $1/2 + \xi$ where the bias ξ vanishes when a security parameter defined by the protocol increases, the task realized is a (*non-exact*) coin tossing. It was found that *exact* coin tossing is impossible [9].

On the other hand, the nonlocal correlation of EPR [12] state has been applied to do much work in quantum information field, such as quantum teleportation and entanglement swapping [13], quantum dense coding [14], QKD [2] and reducing the complexity of communication [15], etc. However, new applications of the EPR state in quantum information field are still to be discovered.

In this paper, we present a quantum coin tossing protocol via entanglement swapping [13] which method has been used in QKD by Cabello [16,17]. This paper is organized as follows. In Section II, we give the framework of our coin tossing protocol, and security of this protocol is analyzed in Section III. In Section IV, we consider the practical situation and discuss the robustness of this protocol. Section V concludes the paper.

II. COIN TOSSING PROTOCOL

At the beginning, Alice and Bob have a pairs of maximally entangled particles respectively. Suppose the initial state of the entangled particles is

$$\left|\Phi^+\right\rangle_{ij} = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)_{ij}, \qquad (1)$$

which is one of the four Bell states. The other three Bell states are

$$\left|\Phi^-\right\rangle_{ij} = \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right)_{ij}, \quad (2)$$
$$\left|\Psi^+\right\rangle_{ij} = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right)_{ij},$$
$$\left|\Psi^-\right\rangle_{ij} = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right)_{ij}.$$

We denote the four Bell states $|\Phi^+\rangle$, $|\Phi^-\rangle$, $|\Psi^+\rangle$ and $|\Psi^-\rangle$ by two classical bits as "00", "01", "10" and "11" respectively. Suppose Alice has particles 1 and 2 and Bob has particles 3 and 4. The four particles are in state $|\Phi^+\rangle_{12} \otimes |\Phi^+\rangle_{34}$. In the next step, Alice sends particle 2 to Bob and Bob sends particle 4 to Alice. Then Alice performs a Bell type measurement on particles 1 and 4 and Bob performs a Bell type measurement on 2 and 3, respectively. According to the theory of entanglement swapping [13], the measurement result will be $\sigma\,|\Phi^+\rangle_{14} \otimes \sigma\,|\Phi^+\rangle_{23}$, where σ is one of the operators of I, X, Y and Z. I, X, Y and Z are defined as

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \quad (3)$$

The two parties will get the same completely random result which is one of the four Bell states (respectively denoted by "00","01","10","11"). If we use "0" to represent "00" or "11" and "1" to represent "01" or "10", this process can be regarded as a simple coin tossing process.

However, only steps mentioned above are not enough to prevent one party from cheating. For example, suppose that Alice wants the result to be "0", she can apply operation I or Y on the particle 4 which is sent out by Bob, then send it back to Bob as particle 2. Otherwise, if she wants the result to be "1", she can apply operation X or Z on particle 4 and send it back.

In the following we give the modification to the naive protocol. Alice and Bob respectively have N pairs entangled particles in the initial. We denote Alice's particles by i from 1 to $2N$, and Bob's particles by j from 1 to $2N$. Alice's $(2m-1)$th and $2m$th particles are entangled in state $|\Phi^+\rangle$, so are Bob's particles. First, Alice sends her particles which are numbered by $2m-1$ ($m = 1, 2, \cdots N$) to Bob with a random sequence not known by Bob. After received all of particles sent by Alice, Bob sends his particles numbered by $2m-1$ ($m = 1, 2, \cdots N$) to Alice in a sequence known by Alice. After received Bob's particles, Alice announces the sequence of practices she has sent to Bob. Then Alice (Bob) performs N times Bell type measurement on the N pairs of her (his) particles, each pair including a particle of herself (himself) numbered by $2m$ and a particle sent by the other party which was numbered by $2m-1$. Both the two parties add their measurement results (e.g. $|\Phi^+\rangle, |\Phi^-\rangle$ are denoted by "0" and $|\Phi^-\rangle, |\Psi^+\rangle$ are denoted by "1"). If the sum is even, the tossing result is "0", otherwise the tossing result is "1". In other words, the tossing result is defined as the total parity bit of the N Bell type measurement results. At the end, the result can be announced to each other participant through public communication channel.

However, only above steps are not sufficient to guarantee the security of this protocol, that is, can not against Bob's cheating. In fact, if Bob wants the result to be "0", he can simply send all Alice's particles back and casually announce Alice a sequence of the particles he send out, without doing anything else. If he wants the result to be "1", he can apply a unitary transformation (X or Z) on any one of particles sent by Alice before sending them back. To check whether Bob has cheated by this means, it requires that Bob announces all his measurement results to Alice. Since that Alice sends particles in the first order, she can not change the probability distribution of Bob's measurement results and needs not to announce her measurement before she knows Bob's results.

III. SECURITY ANALYSIS

Now consider the security of this protocol. Assume that an honest participant should use the value "abort" only if he detects that the other participant has cheated or failed to collaborate. Using the value "abort" at other time is dishonest. It is shown that no secure coin tossing protocol would exist if a protocol could be declared insecure only because a dishonest participant can adopt this abort strategy [9]. Therefore, we don't consider this case.

Before analyzing the security, we give a lemma which will be used later. We define the *parity* of Bell measurement result $|\Phi^+\rangle$ ("00") and $|\Psi^-\rangle$ ("11") be even ("0"), and the parity of $|\Phi^-\rangle$ ("01") and $|\Psi^+\rangle$ ("10") be odd ("1").

Lemma. — Bell type measurement on any two particles among N pairs of particles entangled in EPR state cannot change the total parity of the N pairs of particles.

Proof. — We number all the N pairs of particles from 1 to $2N$, and the $(2i-1)$th particle is entangled with the $2i$th particles. It is obvious that if the measurement on the two particles numbered $(2j-1)$th and $2j$th particles does not change the total parity (where $1 \le i, j \le N$). Without loss of generality, assume that the measurement is on particle $2j-1$ and $2i$ ($i \neq j$). After the measurement, the four-particle ($2j-1$, $2j$, $2i-1$ and $2i$) state will be changed from $|\Phi_1\rangle_{2i-1,2i} \otimes |\Phi_2\rangle_{2j-1,2j}$ to $\sigma\,|\Phi_1\rangle_{2j-1,2i} \otimes \sigma\,|\Phi_2\rangle_{2i-1,2j}$, where $|\Phi_1\rangle$ and $|\Phi_2\rangle$ are any EPR states. Obviously, the total parity of the two new pairs is the same of the two original pairs. Since other particles are not changed, the total parity of the N pairs does not change under Bell type measurement. And we can naturally obtain the below corollary.

Corollary. — Entanglement swapping between any

two pairs among N pairs of EPR states cannot change the total parity of the N EPR pairs.

We consider Alice's strategy first. Since that she sends particles first, no matter what type of state and what sequence she adopts, she cannot change the probabilities of the two outputs of Bob. Suppose the state of the particles Alice sends out is $\rho_{1,3\cdots,2N-1}$ (we have considered the sequence in the subscript) and the state of Bob's particles is $|\Phi^+\rangle^N_{2j-1,2j}$, if Bob projects Alice's particles and his own particles numbered in even numbers onto Bell basis, each projection results will be independently and completely random. The total parity has equal probability to be "0" or "1". Besides, Alice cannot check the credibility of Bob's results. So Alice needs not to cheat by sending fake particles.

There is another question whether she can cheat after Bob sends his particles and the information of the sequence of his particles. For example, she measures her particles and the particles sent by Bob in Bell basis according to the coin tossing rules. Suppose she wants the result to be "0", if she gets the result "0", she announces the true particles' sequence she sent out. Otherwise, she announces another sequence, and expects that Bob's measuring will bring the different result — "1". However, from the lemma, we can deduce that this strategy could not change Bob's measurement result and in fact, there is no way for Alice to change the probabilities of Bob's two outputs after Alice sends out her particles.

Bob has the following strategy. When he receives Alice's particles and should send back his own particles, he can sends back Alice's particles directly if he wants to get the result "0" or he can send them back after applying a X or Z type unitary transformation on any particle if he wants the result to be "1". It can be deduced from the lemma that this strategy will be effective. However, since he must announce the sequence of particles he sends out before knowing the sequence of particles sent by Alice, he can not definitely give the exact results of Alice's all Bell type measurements. What Bob can definitely give out is only the final result — the total parity of all the Bell type measurement results. The average probability that Bob's guess of Alice's measurement results will be pass Alice's test is

$$P = \left(\frac{5}{8}\right)^{N-1}, \tag{4}$$

which exponentially decreases with N increasing. So the bias vanishes exponentially in this coin tossing protocol. The detail procedure to deduce the result of P in Eq. (4) is shown in the Appendix.

IV. ROBUSTNESS OF THE PROTOCOL

Up to this point, we assume that the initial state of a EPR pair is purely in $|\Phi^+\rangle$ and all operations are exact. But in practice, the decoherence of quantum states and errors of operations occur almost all the time. The measurement results of the two parties will not always be consistent since the errors were introduced. If the probability that the inconsistent results arise exceeds the probability in Eq. (4), the protocol becomes useless.

Suppose the probability that a single measurement will get the correct result is Γ, it must satisfy the condition

$$1 - \Gamma^N \leq P. \tag{5}$$

From this equation, it can be concluded that this protocol is very sensitive to error. For example, if $P \leq 0.01$ (that is, $N \geq 11$), it requires that $\Gamma \geq 99.91\%$ with $N = 11$.

V. CONCLUSION

In this QCT protocol, entanglement swapping is used to establish the coincidence of the two participants. The security is guaranteed mainly by the complexity of classical information such as the random sequence Alice uses. In this protocol, when Alice knows the result, she cannot change the result. If Bob tries to cheat, the probability he passes the check is exponentially small, else he cannot change the probabilities of the two outputs. From the above analysis, it can be concluded that though this protocol is not an exact coin tossing protocol, the bias vanishes exponentially.

Acknowledgment

This work was supported by the National Natural Science Foundation of China.

APPENDIX: Deduction of Eq. (4)

Without loss of generality, we only consider the case that Bob wants the result to be "0", and Bob sends Alice's particles back directly after he received the particles. Since Bob does not know the sequence of Alice's particles he received, he can only guess a random sequence and send it to Alice. After Alice announces the sequence that she has sent out the particles, Bob compares this sequence with the sequence he has announced to Alice and makes a set of Bell type measurement results for Alice's check.

Suppose that after comparing the two sequence, Bob finds out that Alice's N pairs of entangled particles can be divided to m ($1 \leq m \leq N$) groups, with each group has some (say $n_k, 1 \leq k \leq M$) complete pairs and (n_k) Bell type measurements, and any group cannot be divided into some subgroups with above properties.

The number of the methods that divide N EPR pairs into m groups is $\begin{pmatrix} N-1 \\ m-1 \end{pmatrix}$. For a group has n_k EPR pairs, the n_k Bell type measurements have definite parity (it can be deduced from the lemma), so the number of all possible measurement results is 4^{n_k-1}. Thus the number of all possible measurement results of the N EPR pairs is 4^{N-m}. Now we can get the average probability that Bob's guess could pass Alice's test

$$P = \sum_{m=1}^{N} \left(\begin{pmatrix} N-1 \\ m-1 \end{pmatrix} \frac{1}{4^{N-m}} \right) / \sum_{m=1}^{N} \begin{pmatrix} N-1 \\ m-1 \end{pmatrix} = \left(\frac{5}{8} \right)^{N-1}.$$

[1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India,* 1984 (IEEE, New York, 1984), p. 175.

[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[3] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **84**, 4729 (2000); D. S. Naik, C. G. Peterson, A. G. White, A. J. Berglund, and P. G. Kwiat, Phys. Rev. Lett. **84**, 4733 (2000); W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, Phys. Rev. Lett. **84**, 4737 (2000).

[4] L. Goldenberg, L. Vaidman and S. Wiesner, Phys. Rev. Lett. **82**, 3356 (1999).

[5] D. Mayers, Phys. Rev. Lett. **78**, 3414 (1997).

[6] H. K. Lo and H. F. Chau, Phys. Rev. Lett. **78**, 3410 (1997).

[7] M. Blum, SIGACT News, **15**, 23 (1983).

[8] H. K. Lo and H. F. Chau, Physica D **120**, 177 (1998).

[9] D. Mayers, L. Salvail and Y. Chiba-Kohno, arXiv: quant-ph/9904078.

[10] S. N. Molotkov, and S. S. Nazin, arXiv: quant-ph/9910034.

[11] A. Kent, Phys. Rev. Lett. **83**, 5382 (1999).

[12] A. Einstein, B. Podolsky and N. Rosen, Phys. Rev. **47**, 777 (1935).

[13] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993); M. Zukowski, A. Zeilinger, M. A. Horne and A. K. Ekert, Phys. Rev. Lett, **71**, 4287 (1993); S. Bose, V. Vedral and P. L. Knight, Phys. Rev. A **57**, 822 (1998); J.-W. Pan, D. Bouwmeester, H. Weinfurter and A. Zeilinger, Phys. Rev. Lett. **80**, 3891 (1998).

[14] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).

[15] R. Cleve and H. Buhrman, Phys. Rev. A **56**, 1201 (1997); P. Xue, Y.-F. Huang, Y.-S. Zhang, C.-F. Li, and G.-C. Guo, arXiv: quant-ph/0012052.

[16] A. Cabello, Phys. Rev. A **61**, 052312 (2000); A. Cabello, arXiv: quant-ph/0009051.

[17] Y.-S. Zhang, C.-F. Li, and G.-C. Guo, arXiv: quant-ph/0009042.